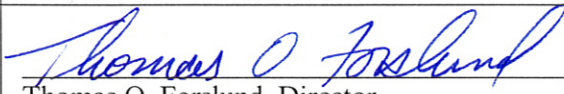
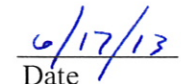


Thomas O. Forslund, Director

Governor Matthew H. Mead

<b>Policy Title:</b>	Contingency Planning
<b>Policy Number:</b>	S-007
<b>Effective Date:</b>	July 1, 2013
<b>Approval:</b>	 Thomas O. Forslund, Director <div style="text-align: right;">   Date </div>

**Purpose:**

The intent of this policy is to ensure contingency plans are in place to support restoration of operations, computing resources, and critical data pursuant to the Wyoming Department of Health (WDH) disaster recovery and emergency mode operation plans.

**Scope:**

This policy applies to all WDH workforce.

**Policy:**

**1. General**

- a. The WDH contingency plan identifies steps that WDH shall take to ensure critical functionality is maintained in the event of loss, disruption, or disaster impacting information systems.
- b. To satisfy contingency planning requirements, the WDH contingency plan shall include:
  - i. Strategies and processes to ensure continuity of information systems;
  - ii. Periodic recovery testing to ensure viability;
  - iii. Processes to store and recover media from offsite storage;
  - iv. Processes to monitor computer and network operations and mitigate interruptions; and
  - v. Recovery tools and offsite facilities to support timely recovery.

**2. Contingency plan.** WDH shall develop a plan to allow physical access to facilities that house protected health information (PHI) in the event of an emergency.

**3. Application and data criticality analysis.** WDH shall assess the criticality of applications, data files, and other contingency plan components by defining the preliminary system information.

- a. Preliminary system information includes:
  - i. System name;
  - ii. Description of the system, including purpose, architecture, and any supporting system diagrams;
  - iii. Division/program/facility name; and
  - iv. Division/program/facility point of contact.
- b. WDH shall characterize the ways both the internal and external point of contact depends on or supports the WDH system or network. Characterization of information may include:
  - i. Name of business associate (external and internal) that provides or receives data from the system;
  - ii. Contacts which support any interconnected systems; and
  - iii. Range of support provided by the system, including:
    - A. Security;

- B. Technical;
    - C. Managerial; and
    - D. Operational.
  - c. WDH shall identify system resources critical to the objectives listed in the emergency mode operation plan. System resources may include:
    - i. Applications;
    - ii. Data files; and
    - iii. Information technology resources.
  - d. WDH shall identify the critical roles of individuals identified in both the emergency mode operation and disaster recovery plans.
  - e. WDH shall determine its recovery priorities based on results of the criticality assessment, and then categorize applications by order of criticality based on:
    - i. Contingency resource allocations and expenditures;
    - ii. Time;
    - iii. Effort; and
    - iv. Costs.
4. **Data backup plan.** WDH shall develop a data backup plan to ensure the availability, integrity, and security of electronic protected health information (ePHI) by:
- a. Identifying critical data files for backup. Critical files shall be identified from the application and data criticality analysis;
  - b. Defining the frequency of full and incremental backups respective to each application and operating system;
  - c. Defining the retention period respective to each application and operating system by taking into consideration the frequency of full and incremental backups for each;
  - d. Identifying systems that require backups and offsite storage location for backups;
  - e. Defining both the individuals who are authorized to request the retrieval of backups and the approved method for transporting backups from the secure facility.
5. **Disaster recovery plan.** WDH shall develop a disaster recovery plan which:
- a. Defines the notification process, including:
    - i. A list of decision-makers; and
    - ii. Identification of the activation team;
  - b. Defines damage assessment processes;
  - c. Defines the procedures for restoring applications and data; and
  - d. Identifies the deactivation team.
6. **Emergency mode of operation plan.** WDH shall identify critical business processes for protecting the security of ePHI while operating in normal mode, and ensure the continuity of such processes while operating in emergency mode.
7. **Contingency plan testing and revision.** WDH shall implement a process for testing and revising contingency plans, including:
- a. Listing elements within the contingency plan that require testing and periodic revision to ensure they remain current and effective;
  - b. Defining the specific objective for each element test and the overall test plan;
  - c. Identifying each test participant and the specific role they are to perform;
  - d. Defining the scenario that will be utilized for each test. Scenarios should include worst-case scenarios, incidents that are most likely to occur, and the time frames and participant(s) associated with each test element;
  - e. Documenting the execution, results of, and lessons learned for each test; and

- f. Revising the plan whenever there are changes affecting:
  - i. Operational requirements;
  - ii. Security requirements;
  - iii. Technical procedures;
  - iv. Hardware, software, and other equipment;
  - v. Facility requirements; and
  - vi. Team members and team members' contact information.

**Contacts:**

De Anna Greene, CIPP/US, CIPP/G, CIPP/IT, WDH Privacy/Compliance Officer, (307) 777-8664  
Tate Nuckols, JD, WDH Security Officer, (307) 777-2438

**Forms:**

SF-001; WDH Contingency Plan Process

**Policies:**

**References:**

45 CFR § 164.308(a)(7)

**Training:**